DETAILED ACTION

Claims 1-35 are pending. Claims 1, 2, 4, 11, and 15-28 are currently amended. Claims 29-35 are new.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 05/08/2008 has been entered.

Response to Arguments

Applicant's arguments, see second paragraph of page 15, filed 05/08/2008, with respect to the rejection(s) of claim(s) 1-28 under 35 U.S.C. 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of a different interpretation of 3GPP TS 33.102 v5.1.0 in view of Bacchus and UMTS Security.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over 3GPP TS 33.102 v5.1.0 (herein 3G Security) in view of Bacchus and UMTS Security.

Regarding claims 1, 15, 24, 25, 26, 27, 28, and 35:

3G Security discloses a method comprising:

sending a request for registration from a user equipment to a serving controller via a second controller, said request for registration including information indicative of at least one security mechanism supported by the user equipment [*page 29 step 2 of figure 14, the MS (mobile station) transfers to VLR/SGSN the initial L3 message*];

determining based on the information in the second controller that the user equipment supports a second security mechanism other than a first security mechanism [*page 29 step 1 of figure 14, the MS transferred the START values and user equipment security capabilities; page 29 step 6 of figure 14, the SRNC decides which algorithm to use out of the user equipment security capabilities*];

including in the request for registration an indication that the second security mechanism is used by the user equipment [*page 30 step 1 of figure14, the UE security capability*]; and

sending a challenge in accordance with the second security mechanism from the serving controller to the user equipment via the second controller [*page 28 last paragraph, figure 14 (steps 1-11) are at initial connection establishment, possible authentication, and start of integrity protection and possible ciphering; page 20 figure 7 shows the generation of the cipher key (CK) and integrity key (IK) using f3 (UEA) and f4*

(UIA) respectively; page 21 figure 8, discloses VLR/SGSN performing and authentication challenge (AUTN) with the USIM (on the user equipment)].

3G Security does not disclose removing the information from the request for registration in the second controller. Bacchus is analogous to 3G security in that they both specify a proxy to select the cipher algorithms from a list. Bacchus discloses a proxy method and system wherein the client transmits the cipher suite list to the proxy [*column 9 lines 25-26*] and the request is forwarded to the server along with the selected cipher [*column 10 lines 16-22; it is implicit that the other ciphers from the list are not sent, therefore they are removed*]. One of ordinary skill in the art at the time of invention could have combined the method of Bacchus with the method of 3G Security in order to forward only the selected cipher to the server [*column 10 lines 16-22*].

3G Security and Bacchus fail to disclose the use of a registration request. UMTS security is analogous to 3G Security as it relates to third generation cellular systems. UMTS Security discloses an IP multimedia subsystem using SIP [*page 199 Section 5-page 200*]. SIP uses registration requests from the user equipment.to the serving controller [*page 202 Figure 7*]. It would have been obvious to one of ordinary skill in the art at the time of invention to add SIP as disclosed in UMTS Security in order to allow for an IP multimedia subsystem [*page 199 Section 5-page200*].

Regarding claims 2, 16, and 29:

3G Security, Bacchus, and UMTS Security disclose a method as claimed in claim 1, further comprising:

forwarding a response to the challenge in a message from the user equipment to the serving controller (page 23 first and second paragraphs, user equipment sends RES (response) to the challenge to VLR/SGSN).

Regarding claims 3, 17, 22, 23, and 30:

3G Security, Bacchus, and UMTS Security disclose a method as claimed in claim 2, further comprising:

using the response for authentication of the message at the serving controller (page 23 second paragraph, if expected response is equal to response, then the authentication of the user has passed).

Regarding claims 4 and 31:

3G Security, Bacchus, and UMTS Security disclose a method as claimed in claim 1, further comprising:

receiving the second controller comprising a network entity providing proxy (page 29 VLR/SGSN performs security functions and access control). UMTS security discloses in figure 7 on page 202 a P-CSCF (corresponding to the VLR/SGSN of 3G Security).

Regarding claims 5 and 32:

3G Security, Bacchus, and UMTS Security disclose a method as claimed in claim 1, wherein the step of sending the request for registration from the user equipment to the serving controller comprises sending a challenge from the serving controller to the user equipment (page 21 figure 8, discloses VLR/SGSN performing and authentication challenge (AUTN) with the USIM (on the user equipment)), sending a response to the

challenge from the user equipment (page 23 first and second paragraphs, user equipment sends RES (response) to the challenge to VLR/SGSN), and registering the user equipment to the serving controller only if a satisfactory response is received from the user equipment (page 23 second paragraph, if expected response is equal to response, then the authentication of the user has passed), and sending a further challenge to the user equipment after the registration step is completed (page 30, the nonce FRESH is sent from the VLR/SGSN to the UE; page 34, FRESH is a network side nonce; it is inherent that the nonce is used as a means of authenticating the MS in order to prevent replay attacks).

Regarding claims 6, 18, and 33:

3G Security, Bacchus, and UMTS Security disclose a method as claimed in claim 1, further comprising: obtaining data for sending the challenge from a user information database (page 41 second paragraph, authentication challenge is retrieved from a local database).

Regarding claims 7 and 34:

3G Security, Bacchus, and UMTS Security disclose a method as claimed in claim 1, wherein the step of sending the challenge comprises sending the challenge comprising an authentication vector (figure 5 on page 18, shows the challenge comprising an authentication vector).

Regarding claims 8 and 19:

3G Security, Bacchus, and UMTS Security disclose a method as claimed in claim 1, further comprising:

providing the first security mechanism comprising a security mechanism in accordance with a Secure Internet Protocol (UMTS security discloses using IPsec (page 203, integrity protection using IPsec ESP).

Regarding claims 9 and 20:

3G Security, Bacchus, and UMTS Security disclose a method as claimed in claim 1, further comprising:

providing the second security mechanism comprising a security mechanism in accordance with a hypertext transfer digest protocol (UMTS security discloses using HTTP Digest (page 202, Authentication using HTTP Digest AKA)).

Regarding claim 10:

3G Security, Bacchus, and UMTS Security disclose a method as claimed in claim 1, further comprising:

sending of at least the challenge or a response in a message in accordance with a session initiation protocol (UMTS security discloses sending the challenge and response in accordance with SIP (pages 202 and 203, Authentication using HTTP Digest AKA)).

Regarding claims 11 and 21:

3G Security, Bacchus, and UMTS Security disclose a method as claimed in claim 1, further comprising:

registering the user equipment with a serving controller of an internet multimedia subsystem (UMTS security discloses registering the UE with a serving controller of an IMS (page 201, Security architecture for the IP multimedia subsystem)).

Regarding claims 12 and 13:

3G Security, Bacchus, and UMTS Security disclose a method as claimed in claim 2, further comprising: including in the request for registration a list of security mechanisms supported by the user equipment (page 29 step 1, MS sends sends the UE security capabilities in a list format); concluding at the second controller based on the list that the user equipment supports the second security mechanism instead of the first security mechanism (page 29 step 4, the VLR/SGSN determines which UIAs and UEAs are allowed to be used in order of preference); an indication that the second security mechanism is to be used (page 30 step 5, the VLR/SGSN orders the list as the most preferable occurring at the top of the list); and forwarding the request to the serving controller (page 30 step 5, VLR/SGSN transmits to the SRNC).

3G Security does not disclose the use of including the lists in the headers. Examiner takes official notice that the use of header information was well known at the time of invention. All the claimed elements were known in the prior art and it would have been obvious to one of ordinary skill in the art at the time of invention to modify the headers to include the lists of security mechanisms in order to inform the receiver of how to handle the data block.

Regarding claim 14:

3G Security, Bacchus, and UMTS Security disclose a method as claimed in claim 3, further comprising:

providing the message comprising a request for a service provided by an application server. It is inherent in an IMS to deliver IP multimedia services to end users [*UMTS Security, page 199 Section 5-page 200*].

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JAMES TURCHEN whose telephone number is (571)270-1378. The examiner can normally be reached on MTWRF 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid can be reached on (571)272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JRT

/Kristine Kincaid/
Supervisory Patent Examiner, Art Unit 2139